



Keyloggers that record your every move online could be installed on your PC without your knowledge. Jon Thompson explains how they work – and how to stop them

Someone, a criminal or a crime investigator, could be watching every move you make on your computer. They don't need cameras or high-tech surveillance gear to do this. All it takes is a tiny little program sitting on your computer, recording every key you tap on your keyboard. These programs, called keyloggers, send back the information they gather to their creator. This is great for society if they're logging a mafia mastermind or al-Qaida cell member, but not so great if the keylogger was created by a criminal wanting your credit card details.

According to an ABC News investigation carried out late last year, keylogging, which is the act of capturing keystrokes to gain private credentials, now plays a part in a third of all computer crime, second only to botnet-based extortion (explained below). As people run their lives from home PCs, bank accounts have started emptying and credit card bills growing.

For some law enforcement agencies, keylogging is fast becoming an important weapon in their arsenal against organised crime and terrorism. Worried parents have also started using keyloggers to check up on their children's online activities. Employers too are free to log the keystrokes you make on their time and on their computers. But it's the risk posed by the illegal use of these practically undetectable programs that causes most harm to the individual. For the fraudster, keyloggers are

the high-tech equivalent of looking over your shoulder as you enter your PIN at a cashpoint. Do you know who's watching you as you surf the internet?

WATCHING THEM, WATCHING YOU

According to cyber-security company iDefense, the number of malicious keylogging programs in the wild rose over 65 per cent in 2005 and this year seems as if it will top that by a considerable margin. Best estimates claim there are 6,200 variations on a theme already roaming free in cyberspace. Computers infected with illegal keyloggers watch everything you do. Once triggered they send the keystrokes, including any personal credentials, to a central server for later use or sale.

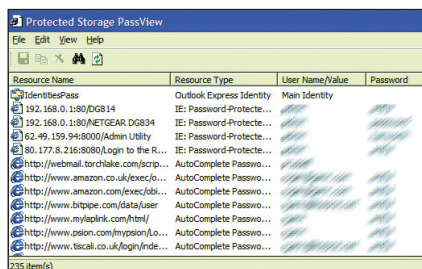
The distribution of malicious keylogging software usually takes place via virus-infected email attachments, but unpatched browser flaws can just as easily infect a computer simply by the user visiting dubious websites. Online security company SecurityFocus maintains a publicly accessible vulnerability database (www.securityfocus.com/bid) that, at the time of writing, lists 64 security flaws in the latest version of Microsoft's Internet Explorer web browser. Several of these are suitable for deploying code directly on the surfer's computer without their knowledge, and certainly without their permission. Add to this a cavalier attitude about having up-to-date anti-virus and spyware

protection, and conditions are ripe for infection and potential financial meltdown. The problem is that without dedicated, up-to-date detection software, keylogger infection is also uniquely difficult to spot.

While botnets involve hackers controlling thousands of unwitting PCs and using them to bombard victims with an onslaught, keyloggers are frugal in their needs. They hide themselves away and just copy every piece of interesting information to an equally hidden file, so their core functionality is surprisingly simple. Some, including legitimate, commercial offerings, can remove themselves from the running process list. But it's when someone starts using the collected data that the real fun starts.

STEALTH IS THE KEY

The victim might eventually notice that the websites they use have last login times that don't correspond to their visits, and even contain offensive posts they never made. Depending on what the author or distributor of the keylogger has in mind, unauthorised charges might begin appearing on the victim's credit cards for goods they didn't order. Prosecution becomes more difficult if the delivery address is in a different part of the world. Because most people only get monthly bank and credit card statements, keylogging fraudsters have a potential window of opportunity of several weeks in which they can avoid detection.



▲ The Protected Storage Area contains private data that can be accessed by the keylogger

Because of this, it is more important than ever to check email regularly and pay particular attention to emailed receipts from online payment services and commercial websites. The keylogging fraudster's fun doesn't stop there, however. He can sometimes see credentials entered and stored by your web browser before infection ever took place.

A Windows XP keylogger might also have access to data retrieved from part of the system called the Protected Storage Area (PSA). This contains auto-fill data that the user has saved for convenience, including usernames and passwords. The system holds this data securely but, when required, plays it back as if typed in on the keyboard. Any data that populates an input box is open to the keylogger, whether via the keyboard or replayed from the PSA. Tools such as Northwest Performance Software's NetscanTools Pro (<http://tinyurl.com/8ej48>) dramatically show what credentials a keylogger can see by displaying the unencrypted contents of the PSA.

Mozilla Firefox users can breathe a small sigh of relief because this browser does not use the PSA to store credentials and does not suffer from the same bugs as Internet Explorer.

However, this mitigates the threat only slightly, because keylogging still catches everything the Firefox user types. Entering key presses by clicking the mouse on an onscreen keypad, such as when using VoIP applications, is also vulnerable to keyloggers that are capable of monitoring virtual keyboards. Data sent over an encrypted https:// link isn't safe either, because keyloggers capture keystrokes at source, before subsequent encryption takes place.

But keyloggers haven't always had such a bad reputation. In fact, they started off with another purpose entirely.

TESTING TIMES DETECTING CRIMES

Originally, keyloggers were programs designed to capture everything about the way people used software packages during development and testing. Capturing exactly what a tester was doing when a problem occurred saves debugging time later by removing the need to rely on faulty human recall. In testing multi-user software, timing might be crucial too, so exact information is important in re-creating the circumstances that led to a problem. Replaying the tester's actions can instantly replicate the original conditions to test subsequent bug-fixing. GUI designers also need to know how people use software, which functions they use the most and in what order, so they can create and tweak better user interfaces. Beyond this, however, the legitimate use of keylogging seems to have become dubious.

What worries many privacy campaigners is secret keylogging, where the user has no knowledge of such activity. The number of available packages has soared in recent years, as has their use, including by home users. As parents gain better practical understanding of computers and the potential risks to their

children, some have started to monitor their children's online lives, ostensibly to keep them from harm (see the box opposite). A quick web search shows that perfectly legitimate, commercial keylogging software is freely available for download. What's more, the UK's Misuse of Computers Act says nothing against keylogging on a computer you own, unless you use the information you gather to commit crimes such as fraud, or to break into and damage a system you don't own.

At work, where the normal laws on privacy are subject to contract and policy, employers too have begun using keyloggers to weed out illegal activity. Perhaps most controversial, however, is the security services' use of the technology. Magic Lantern, developed and used by the FBI, is one such piece of software (see the box below).

THE ENEMY WITHIN

While the personal cost to an individual who suffers a malicious keylogger infection can be great, in the right hands the sheer size of the crimes made possible by the use of such software is breathtaking. Last year, for instance, detectives from the National High Tech Crime Unit thwarted a massive theft at the London offices of the Japanese-owned Sumitomo Mitsui bank. The intention had been to steal £220 million; had the gang pulled it off, this figure would have dwarfed the UK's current largest robbery of £53 million.

The Sumitomo Mitsui plan called for nearly a dozen electronic transfers of cash into separate bank accounts in different countries, but the gang first needed to gain what looked like legitimate access to the bank's network. What better way than to use legitimate user credentials? When first detected, it looked as if there had been a very clever and sophisticated

Tapping the networks Carnivorous computing

Security services once tapped the phone lines of terrorists and organised criminals to gather evidence against them. But in today's high-tech world, email is as big a part of people's lives as the telephone.

Though now supposedly retired in favour of commercial packages, the FBI's shadowy Carnivore system was the first publicly exposed 'policeware' system to sit on the network at an ISP and sniff packets just as a phone tap could. Though exposed in 2001, this wasn't the first time the FBI had used software to spy on suspects.

In an affidavit filed in the US Supreme Court in October 2001, FBI deputy assistant

director Randall Murch admitted the bureau had officially used keylogging in 2000. A New Jersey loan shark and gambling racketeer called Nicodemo Scarfo Jr received a lengthy jail sentence after agents broke into his office and secretly installed a keylogger on his computer. This enabled them to capture encryption keys to decrypt emails and gather evidence against him.

The FBI planned enhancements to the original Carnivore system, under the code name Cyber Knight. In 2001, the Electronic Privacy Information Center got wind of these enhancements and filed a request under the US Freedom of Information act to find out more. Despite having large areas blacked out, the declassified documents they received showed one such enhancement to be a keylogger called Magic Lantern, the existence of which the FBI confirmed publicly on 12th December 2001.

Despite stories that Carnivore is retired, Magic Lantern lives on and, in a world where enemies of the state no longer wear uniforms, many see such techniques as a legitimate way to prosecute in the war on terrorism. The only problem has been how to deploy keyloggers in ways that stand up in court.

As with the Scarfo case, agents could install a keylogger after gaining physical access to the

system, but a defence counsel could argue that along with the software they had also planted evidence. The Feds needed a method of infection above reproach. According to a report into Carnivore by MSNBC's Bob Sullivan, in most cases they just need to send an email claiming to be from someone known to the suspect. Criminal masterminds are as susceptible to opening enticing attachments and infecting their systems as the rest of us.

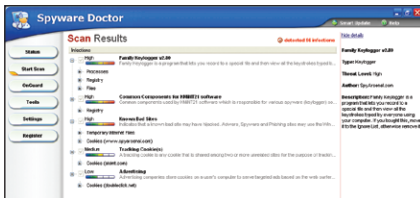
Magic Lantern records instant messaging and chatroom traffic and can even detect the numbers entered on a VoIP keypad. Because of this, agents can still build up a picture of a criminal organisation even if they can't hear the actual words spoken.

More controversial than the deployment of snooping software by the security services are the public announcements by some anti-virus companies that they will ignore Magic Lantern-like systems while still detecting other keyloggers. One that has explicitly refused, however, is UK-based Sophos.

"Malicious code is malicious code," said Graham Cluely, senior technology consultant for Sophos, when Magic Lantern first became public knowledge. "If a customer suspects they may be under surveillance and sends a Trojan horse to us, we're going to provide protection against it."



▲ UK-based Sophos seeks to provide protection against all keylogging Trojans



▲ Spyware Doctor lists all kinds of cookies and Trojans and measures their threat level

breach of electronic security from the outside, but as the investigation progressed, it emerged that the crime had also involved a breach of trust by employees using a keylogger. At the time Dan Morrison, a fraud partner at London law firm Mishcon Del Reya, told the BBC, "I'm struggling to think of a fraud case I've ever done which didn't involve an insider. It's not just access that's needed; it's understanding."

By exploiting quirks in the bank's practices and networks, the crooks, with inside help, deployed keyloggers on the bank's connection to the SWIFT network, used to perform international money transfers. Access to this meant they could freely transfer money to anywhere in the world. It would have worked, too, were it not for a suspicious employee raising the alarm. Police in Tel Aviv arrested one of the gang, Yeron Bolondi, and charged him with money laundering and deception after someone at the bank queried a suspicious transfer of £13.9 million into an Israeli bank account. This may be just the start of a new trend in high-tech bank robbery.

According to anti-spyware company Webroot (www.webroot.com), keyloggers could already infest up to 15 per cent of all corporate PCs, which is frightening enough for system administrators. But it could also mean a future filled with more opportunities such as the one exploited at Sumitomo Mitsui Bank.

Luckily, dedicated anti-spyware systems are good at detecting keyloggers. Regular updates prevent infections by new variants. After installing firewall, anti-virus and even intrusion-detection systems, anti-spyware represents a necessary fourth line of online defence.

As people depend more and more on cyberspace to run their lives, there's a clear need to keep abreast of the latest threats. Whether it is a good idea to ignore official uses of keyloggers, however, is less clear. **CS**

Honey I spied on the kids Interview with a logger

Increasingly, children, and teenagers in particular, are far more at home online than their parents are. The opportunities to converse with other youngsters who share their interests make for a liberating experience. But some parents fear the worst, and a few have even chosen to monitor their offspring's online activities in an attempt to keep them safe.

Computer Shopper talked to Stephen (not his real name), who decided to install a keylogger about six months ago to ensure that his daughters, aged 11 and 14, and son, 16, remained safe online. His children don't know about this, so why did he choose to take such drastic action?

"It was not an easy decision to make, but a major part of it was not knowing what they were getting up to on the computer, which was a worry to [me and my wife]. You can't be there all the time, and the news was full of stories about kids going to meet people they had met online. We just felt it was safer to know what they were up to. When they're out we insist on them telling us where they are, and we ring other parents to check on them, so really it was just an extension of that."

So how did he go about it? "We just downloaded a keylogger and installed it on the family computer in the living room. It has a special combination of keys you have to press to get the Control Panel up and then you can look at the log to see what's been going on."

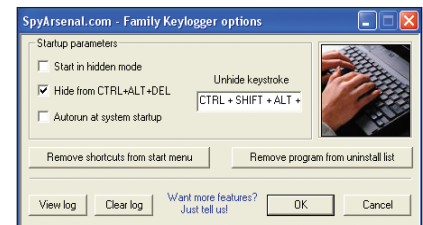
But isn't logging everything his kids type to their friends a breach of trust? "Initially, I felt bad and we talked about it a lot, but we came to the conclusion that we'd rather say sorry and explain why we did what we did than have something bad happen to one of them."

And what do they get up to online? "I don't want to say, but it's not anything bad. I just want to know that they're not up to anything really dreadful or falling in with the wrong crowd. I delete the log file immediately after I've read it and forget about it."

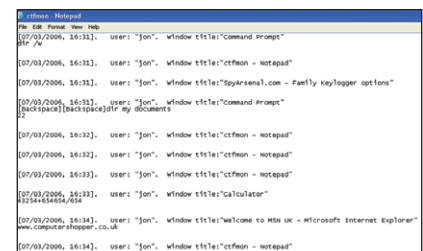
What would Stephen do if he found that something was going on that he thought might be dangerous? "Well, we're hoping that never happens. But if and when it does, we'll explain what we've done and why we did it. If one of our children ever finds out about what we've been doing, we will sit them down as a family and tell them that we only wanted to protect them because we love them. We think they'll understand why."

Wouldn't it be better simply to educate his children about the risks of life online and to trust them? Stephen is adamant. "We believe this gives them the most freedom to explore without them knowing that we are keeping them safe. Do you want to be making an appeal when one of your kids goes missing? I certainly don't."

It's a controversial idea, but one Stephen feels is worth the risk. "I do worry about them finding out, but at the end of the day it's about us loving them and wanting them to stay safe. The internet is a great place, but there are people out there from whom we need to keep our kids safe."



▲ Keeping tabs on a child's movements online using Family Keylogger could keep them safe, but at what cost to the trust they have in you?



▲ Keylogger output gives parents a detailed record of every keystroke made by their child

Key to the law The Computer Misuse Act

In the UK, the 1990 Computer Misuse Act is the law that provides for the prosecution of online criminals, but what does it say? Can you use a username and password you happen to know if it gets the job done when the owner isn't around? Can you install a keylogger on your own system to secretly track its use by others? Is it OK to do so on a system used by employees? To answer such questions, it's necessary to delve into the act's three sections.

The legislation breaks into three parts, each describing an offence more serious than the last and carrying heavier penalties. Section one covers unauthorised access to a computer. Under it, you commit an offence if you cause a computer to give you access that you would not normally have. This clearly

covers hacking, but also makes it an offence to use someone else's login details without permission. The maximum penalty for a crime prosecuted under this first section is currently six months in prison and a £5,000 fine.

The second section expands on section one with the more serious offence of gaining unauthorised access to a computer with the intent of carrying out a further crime. Cases brought under this section go to the Crown Court and carry a maximum sentence of five years plus a hefty fine.

The final section concerns the making of unauthorised changes to or destruction of the data or programs stored in a computerised system itself. This is the most serious of the three offences as it undermines the integrity of the system itself. Cases brought under this

section go to the Crown Court and carry a maximum sentence of five years and a fine.

In 2004, the All Party Internet Group tabled amendments to the Computer Misuse Act, including an increase in sentences and explicitly outlawing the rising tide of denial-of-service attacks. Sadly, the parliamentary session ended before amendments gained royal assent into law. In the UK, this means the process must begin again rather than picking up where it left off during the next parliamentary session.

Despite the law, prosecutions remain pitifully infrequent. During the period 1998 to 2002, Home Office figures show that prosecutions brought under sections one, two and three totalled just 33, 22 and 36 respectively. That's a total of just 91.